Supreme Court, U.S.
FILED
APR 27 2000
OFFICE OF THE CLERK

(1)

No. 00 17

IN THE

Supreme Court of the United States

ARABIAN SHIELD DEVELOPMENT COMPANY
Petitioner

v.

CENTRAL INTELLIGENCE AGENCY

On Petition for Writ of Certiorari
To the United States Court of Appeals
For the Fifth Circuit

PETITION FOR WRIT OF CERTIORARI

MICHAEL CRISSMAN LAWRENCE
Counsel of Record
BEENE & LAWRENCE, P.L.L.C.
5949 Sherry Lane, Suite 800
Dallas, Texas 75225
TEL: (214) 346-2630
FAX: (214) 346-2631
Counsel of Record for Petitioner Arabian Shield Development Co.

101pp

QUESTIONS PRESENTED FOR REVIEW

I. Should the Central Intelligence Agency ("CIA") have conducted a balancing test pursuant to Executive Order 12958 before it denied Petitioner Arabian Shield Development Company's ("Arabian Shield") Freedom of Information Act requests?

II. Did the district and appellate courts commit reversible error when they granted/affirmed CIA's motion for summary judgment and denied Arabian Shield's motion for summary judgment because they shifted the burden of proof from the CIA to Arabian Shield to prove that the CIA classified its documents "in order to" conceal criminal acts?

III. Did the district and appellate courts commit reversible error when they granted/affirmed CIA's motion for summary judgment and denied Arabian Shield's motion for summary judgment because Executive Order 12958 prohibits the classification of national security information "in order to" conceal a crime?

CORPORATE DISCLOSURE STATEMENT

Petitioner Arabian Shield Development Company does not have a parent company, and no publicly held company owns 10% or more of its stock.

TABLE OF CONTENTS

Questions Presented for Review i

Corporate Disclosure Statement ii

Table of Authorities iv

Citations to Opinions/Orders 1

Jurisdictional Statement 2

Statutes/Executive Orders at Issue 2

Statement of the Case 3

Argument 6

Appendix 19

TABLE OF AUTHORITIES

Cases **Page**

Central Intelligence Agency v. Sims,
471 U.S. 159 (1985) 14, 16, 17

Vaughn v. Rosen,
484 F.2d 820 (D.C. Cir. 1973), *cert. denied*,
415 U.S. 977, 94 S.Ct. 1564,
39 L.Ed.2d 873 (1974) 11, 13

Statutes

5 U.S.C. § 552 ..... 3, 5, 8, 11, 12, 13
15 U.S.C. § 78-dd 3, 8
50 U.S.C. § 403-3 14

Miscellaneous Authorities

Executive Order 12958 4-17

CITATIONS TO OPINIONS AND ORDERS
BY THE ADMINISTRATIVE AGENCY AND COURTS

1. January 23, 1998 CIA response to Arabian Shield's August 8, 1997 Freedom of Information Act request.

2. June 30, 1998 CIA response to Arabian Shield's October 8, 1997 Freedom of Information Act request .

3. February 26, 1999 Judgment from the United States District Court for the Northern District of Texas in Cause No. 3-98-CV-0624-BD (judgment entered March 1, 1999).

4. February 26, 1999 Memorandum Opinion and Order from the United States District Court for the Northern District of Texas in Cause No. 3-98-CV-0624-BD (entered March 1, 1999).

5. January 28, 2000 Judgment from the United States Court of Appeals for the Fifth Circuit in Cause No. 99-10327 (entered January 28, 2000).

JURISDICTIONAL STATEMENT

1. The United States Court of Appeals for the Fifth Circuit entered its judgment on January 28, 2000.

2. This Petition for Certiorari was served on the Clerk of the United States Supreme Court on or about April 27, 2000 but was returned to Petitioner on or about May 3, 2000 for reformatting pursuant to Supreme Court Rule 14.5.

3. This Supreme Court of the United States has jurisdiction of this matter pursuant to 28 U.S.C. §. 1254(1).

CITATIONS TO STATUTES AND EXECUTIVE ORDERS AT ISSUE

1. 5 U.S.C. § 552

2. Executive Order 12958

STATEMENT OF THE CASE

This proceeding is an appeal under the Freedom of Information Act, 5 U.S.C. § 552 ("FOIA"). Petitioner Arabian Shield Development Company ("Arabian Shield") submitted two requests for information under the FOIA to the Central Intelligence Agency ("CIA"). The first request was dated August 8, 1997 (Appendix 18-19). After all administrative procedures were exhausted, the CIA made its final response to this first request on January 23, 1998 (Appendix 20-22). On October 8, 1997, Arabian Shield filed the second request for information under the FOIA with the CIA (Appendix 23-26). After all administrative procedures were exhausted, the CIA made its final response to this second request on June 30, 1998. (Appendix 27-30).

Arabian Shield's two FOIA requests consist of several parts. However, the substance of the two requests seeks information pertaining to an oil production sharing agreement with the then existing country of the Yemen Arab Republic. The production sharing agreement was negotiated in 1981, and the two FOIA requests relate to events from 1981 through 1983. The two requests and the administrative processing and appeals of the two requests make clear that Arabian Shield has some evidence that the government of the Yemen Arab Republic was bribed to award the production sharing agreement to a U.S. competitor of Arabian Shield: Hunt Oil Company of Dallas, Texas.

Arabian Shield placed the CIA on notice that it believed that there had been a violation of the Foreign Corrupt Practices Act, 15 U.S.C. § 78-dd, *et seq.*, and that Arabian Shield had on file with the U.S. Department of Justice a complaint under that Act.

The CIA's final reply to both of Arabian Shield's FOIA requests was substantially the same. By letter dated January 23, 1998, the Agency Release Panel, the internal appellate body of the CIA for dealing with FOIA requests,

rejected the first of Arabian Shield's requests with the following language:

> Mr. McNair has determined that the fact of the existence or nonexistence of any documents which would be responsive to your request is classified pursuant to Executive Order 12958. Further, the fact of the existence or nonexistence of such documents would relate directly to information concerning intelligence sources and methods which the Director of Central Intelligence has the responsibility to protect from unauthorized disclosure in accordance with Subsection 102(d)(3) of the National Security Act of 1947 and Section 6 of the Central Intelligence Agency Act of 1949. Accordingly, pursuant to Freedom of Information Act exemptions (b)(1) and (b)(3), your appeal is denied. (Appendix 29-30).

Arabian Shield's second FOIA request was finally denied by letter dated June 30, 1998, giving substantially the same reasons for denying the first request. (Appendix 27).

This appeal deals with internal conflicts within the provisions of Executive Order 12958 ("E.O. 12958;" Appendix 43-80), the applicable Presidential order governing the classification of national security information by the various Executive Branch agencies involved in intelligence gathering. Arabian Shield argues that Section 1.8 of E.O. 12958 is a policy-based prohibition against classifying information in order to conceal a violation of law; in this case the Foreign Corrupt Practices Act, *supra*. Arabian Shield also argues that under the provisions of E.O. 12958, the CIA is required to apply a balancing test when presented with a FOIA request for information, weighing the policy set out in Section 1.8 against the risks of

compromising intelligence sources and intelligence gathering methods.

It is uncontested in this matter that the CIA has not reviewed the contents of any documents that might be responsive to Arabian Shield's FOIA requests. The CIA has not applied any form of balancing test to determine if, in its internal judgment, any part of the information it may have that would be responsive to Arabian Shield's FOIA requests can be released without undue risk to intelligence sources and gathering methods.

At the current state of the facts in this dispute, Arabian Shield seeks a remand of this matter to the District Court with instructions that the CIA review the contents of its files and make an internal determination including the policies set out in Section 1.8 of E.O. 12958.

Arabian Shield appealed the CIA's administrative decision to the United States District Court for the Northern District of Texas, Dallas Division. The United States District Court for the Northern District of Texas had jurisdiction of this matter pursuant to 5 U.S.C. Sec. 552, ¶ 4(B), Freedom of Information Act, in that Arabian Shield appealed an adverse ruling after exhausting its administrative remedies. The matter was submitted to the District Court on opposing motions for summary judgment. On February 26, 1999, the District Court sustained the CIA's motion for summary judgment and overruled Arabian Shield's motion for summary judgment. (Appendix 7-17). Arabian Shield appealed the judgment of the United States Court of Appeals for the Fifth Circuit. On January 28, 2000 the Court of Appeals issued its ruling affirming the District Court's judgment. (Appendix 1-4) Arabian Shield is appealing the Court of Appeals' decision.

ARGUMENTS AND AUTHORITIES

I. The district court erroneously granted CIA's motion for summary judgment and denied Arabian Shield's motion for summary judgment because the CIA failed to conduct a balancing test pursuant to Executive Order 12958 before it denied Arabian Shield's Freedom of Information Act requests.

A. Executive Order 12958 contains inconsistent provisions

The crux of the dispute before this Court lies in conflicts among several provisions of Executive Order 12958, the applicable version of the Presidential order that promulgates and regulates the secrecy of national security information gathered and owned by the United States Government. The preamble to E.O. 12958 states, "This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information." E.O. 12958 constitutes not only an independent grant of authority by the Executive Branch for secrecy and classification but also the implementing rules and criteria for what may be classified and what may not be classified by Executive Branch agencies under both Executive and Legislative authority, E.O. 12958 § 1.2.

Within E.O. 12958, there are specific criteria for what may be classified, for what steps shall be taken when a request for information is received under the Freedom of Information Act, and an express prohibition against classifying certain types of information. In this matter, the CIA is relying on certain provisions of E.O. 12958 to shroud in legal secrecy any information it may have. Specifically, the CIA points to E.O. 12958 § 1.5(c), which authorizes the classification of "...intelligence activities..., intelligence sources or methods...." Additionally, the CIA relies on E.O.

12958 § 3.7(a), which provides:

> 3.7. Processing Requests and Reviews. In response to a request for information under the Freedom of Information Act... (a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

Arabian Shield, on the other hand, is relying on a specific provision of E.O. 12958 which prohibits the classification of information in order to conceal the commission of a crime. E.O. 12958 § 1.8, provides as follows:

> 1.8. Classification Prohibitions and Limitations. (a) In no case shall information be classified in order to: (1) conceal violations of law... .

Under the facts of this case, these internal provisions within E.O. 12958 are in conflict. This internal conflict among the provisions of E.O. 12958 presented in this appeal appears to be a case of first impression. Arabian Shield's research has found no cases that have dealt with this issue nor any closely parallel issues.

B. Executive Order 12958 requires the CIA to review the "contents" of its documents to determine whether they contain information pertaining to the violation of a U.S. criminal statute.

The conflict that is now before this Court began as two requests for information under the Freedom of

Information Act, 5 U.S.C. § 552. A review of the information provided in the FOIA request proceedings and of the Affidavit of Hatem El-Khalidi in support of Arabian Shield's Motion for Summary Judgment in the district court clearly makes three points:

(1) The FOIA requests are directed at a narrow, precise set of events expressly involving the possibility of the crime of bribery of a foreign government official;

(2) Arabian Shield has a good faith basis to believe that there are reports or other documentary information pertaining to the FOIA requests; and

(3) Arabian Shield does not actually know what documentary information, in fact, exists nor what the content of such documentary information might be.

From the very beginning, Arabian Shield has pointed out to the CIA that its inquiry related to a possible violation of the Foreign Corrupt Practices Act and related to a complaint under said Act on file with the U.S. Department of Justice. Arabian Shield does believe, based on a good faith basis, that the ***content of the documents*** that it believes should exist in the CIA files is reasonably calculated to reveal relevant evidence of the bribery of a foreign government official, a violation of the Foreign Corrupt Practices Act, 15 U.S.C. § 78dd-2.

Arabian Shield's requests under the FOIA triggered mandatory declassification reviews of the information sought, if any exists, under E.O. 12958. See Sections 3.6 and 3.7 of E.O. 12958. The CIA, however, has stated under

oath that its information officer processing Arabian Shield's FOIA request did not read or review any documents in formulating his response and did not look to see if there were documents that would contain information that might be responsive to Arabian Shield's requests. In the Second Declaration of William H. McNair Information Review Officer, Directorate of Operations, Central Intelligence Agency, Mr. McNair testifies as follows:

> In making this classification decision, I considered only the classification categories and standards for classifying information contained in E.O. 12958. No part of my analysis included the concept of concealing violations of law. ***In fact, I do not know whether or not responsive documents exist.*** [emphasis added] (Tr. Vol. 1, p. 198).

No one has looked to see if there are documents that would be responsive to Arabian Shield's FOIA requests. No one has reviewed the content of any such documents to determine if they contain information pertaining to the violation of a U.S. criminal statute. Arabian Shield cannot. The CIA has not.

The conflict here is apparent. Arabian Shield seeks to focus E.O. 12958 § 1.8, on the ***content*** of those reports or other documentary evidence which it believes exist. If the content shows evidence of a violation of the Foreign Corrupt Practices Act, then Arabian Shield urges a balancing test must be applied to determine if information can be released using tools such as redaction, excerpting, or partial information release. The CIA, on the other hand, focuses on the ***source*** of the information sought (if any exists). If the source is itself classified, as determined at the time of the FOIA request, then the CIA urges that it need not go further into the content (if any).

The apparent policies behind the parties' positions

are also in conflict, and both policies are valid. The CIA does not and has not asserted that national security secrecy should be used "...in order to..." conceal a violation of law. Arabian Shield does not and has not asserted that the safety and effectiveness of intelligence sources and methods should be compromised by revealing same in response to FOIA requests.

However, it is premature to conclude that the conflict between these positions is irreconcilable. Since the CIA itself has not looked at the content of any documents (if any exist) to determine if they contain information responsive to Arabian Shield's FOIA requests, there are two things which the CIA cannot, at this time, state: (1) that revealing redacted or excerpted information or revealing parts of the information found would compromise sources or methods of intelligence gathering, and (2) that E.O. 12958 § 1.8, has been considered and complied with in making the FOIA classification or declassification decision. A stepped process of examination and review should be the answer. This process will be discussed in more detail under Section IV regarding remedies sought.

II. The district and appellate courts erroneously granted/affirmed CIA's motion for summary judgment and denied Arabian Shield's motion for summary judgment because the courts shifted the burden of proof from the CIA to Arabian Shield to prove that the CIA classified its documents "in order to" conceal criminal acts.

Section 1.8(a)(1) of E.O. 12958 reads, "...In no case shall information be classified ***in order to*** (a) conceal violations of law... ."[emphasis added]. In the trial court, the CIA pointed to this emphasized language and argued that to trigger Section 1.8(a)(1), the CIA must having a knowing intent to conceal evidence of a crime. The trial

court agreed, and in his Memorandum Opinion and Order stated as follows:

> Section 1.8 thus prohibits an agency from classifying documents as a ruse when they could not otherwise be withheld from public disclosure. It does not prevent the classification of national security information merely because it might *reveal* criminal or tortious acts. Plaintiff has neither argued nor offered evidence that the CIA classified the requested information for the purpose of concealing a crime. (Appendix 7-17).

The subject language, "in order to," clearly involves some level of intent. However, Arabian Shield argues that (1) Section 1.8 does not require a knowing intent to conceal to trigger its prohibitions against classification, and (2) the trial court misplaced the burden of proof under Section 1.8. Again, Arabian Shield's research has found no cases construing Section 1.8 of E.O. 12958 nor the phrase "in order to." Arabian Shield would suggest that this phrase, "in order to", is an ambiguous term as used.

Before looking to possible meaning of "in order to," Arabian Shield would point to the trial court's misplacement of the burden of proof. As quoted above, the trial court stated, "Plaintiff has neither argued nor offered evidence that the CIA classified the requested information for the purpose of concealing a crime."

The FOIA places the burden of proof for an exception to the FOIA on the agency claiming the exception; in this case, the CIA. *See,* 5 U.S.C. § 552(a)(4)(B); *Vaughn v. Rosen*, 484 F.2d 820, 823 (D.C. Cir. 1973), *cert. denied*, 415 U.S. 977, 94 S.Ct. 1564, 39 L.Ed.2d 873 (1974). There is nothing in the statute that would place any part of the burden of proof on the citizen seeking information under the FOIA. Additionally, E.O. 12958 defines an FOIA request as

an event calling for a mandatory declassification review by the affected agency, E.O. 12958, Secs. 3.6, 3.7. Since the issue is classified, confidential information, there is no way the requesting citizen can make a determination that information that conceals information of a crime is being secreted in possible violation of Section 1.8. By the very nature of the FOIA, as used in this case, Arabian Shield could not and cannot offer evidence that the information sought results in the concealment of information of a crime. The evidence is secret and in the hands of the government agency. To place any part of the burden of proof on Arabian Shield would render Section 1.8 a nullity, or at least unreviewable. Clearly, the FOIA, E.O. 12958, and the availability of evidence mandates that the burden of proof is on the CIA to demonstrate that it classification decision complies with E.O. 12958; especially Section 1.8.

Arabian Shield refers the Court to the FOIA § 552 (b)(1)(B), which requires that information withheld as classified must be "...in fact properly classified pursuant to such Executive order... ." Section 1.8 of E.O. 12958, by its terms, is not some form of confession in avoidance. It is a policy-based prohibition against secreting certain categories of information, and it prohibits classification of these categories of information no matter what other countervailing considerations may exist. Again, there are no cases on point, but the language of Section 1.8 is clear and direct.

As noted above, at the present time the CIA cannot state that the classification of any information contained in its files which might respond to Arabian Shield's FOIA requests complies with Section 1.8 of E.O. 12958. That is because the CIA has not looked. The CIA intentionally does not know if the result of its actions is to conceal evidence of a crime. It would appear to Arabian Shield that if the CIA does not know, by its own choice, whether or not the result of its classification decision is to conceal evidence of a crime, then it can hardly carry its burden of proving that the

information in question was not classified "in order to" conceal a crime. Additionally, Arabian Shield would argue that both the FOIA and E.O. 12958, §§. 3.6 and 3.7, require that the CIA look and know the impact of its classification decision. Pursuant to *Vaughn*, a government agency is required to formulate a system of itemizing and indexing that would correlate each document or part of a document the agency sought to withhold with the specific justification for withholding. *Id.* at 827.

The CIA, on the other hand, seems to be arguing that once it determines that responding to Arabian Shield's FOIA requests might compromise intelligence sources or gathering methods, it need look no further. If that is the law, that eliminates any possibility that redacted, excerpted, or partial responses could be made without so compromising or unduly compromising sources or methods. Redaction, excerpting, and partial responses are common tools used when dealing with confidential or privileged information. The CIA's position would make those tools unavailable for responses to FOIA requests. *Id.* at 825.

As the Court can see, the phrase "in order to" as used in Section 1.8 is not clear. However, under the facts of this case, the question of the CIA's intent is not really reached. The CIA itself is ignorant of the impact of its decision to deny Arabian Shield's FOIA requests and cannot state any intent or lack of intent pertaining to it classification decision.

Later, perhaps, after the CIA has reviewed the content of documents that might be responsive to Arabian Shield's FOIA requests, the question of the phrase "in order to" might arise again. It is certainly possible that the CIA might make an informed decision that, on balance, it still cannot respond to the FOIA requests in question without revealing sensitive information. Then and only then would the courts be faced with the choice of requiring some level of in camera review of documents as expressly allowed under the FOIA, 5 U.S.C. § 552(4)(B). However, before the issue

of an in camera review were to present itself, CIA professionals would be called on to determine if any information could be released, and one must presume that they would do their job in compliance with the governing Executive Order and the spirit of the FOIA. In other words, if the CIA were to look at the content of the documents in question, the issue might prove to be moot.

III. The district and appellate courts erroneously granted/affirmed CIA's motion for summary judgment and denied Arabian Shield's motion for summary judgment because Executive Order 12958 prohibits the classification of national security information "in order to" conceal a crime.

There are several cases interpreting the rights and duties of the CIA when dealing with national security secrecy. These cases are only partially on point. None of them deal with Section 1.8 of E.O. 12958, and none of them interpret the phrase "in order to" used in Section 1.8. However, since the first level of remedy sought by Arabian Shield before this Court is to have the CIA itself review the content of documents that might be responsive to Arabian Shield's FOIA requests, these cases support Arabian Shield's position in this appeal.

The lead case is *Central Intelligence Agency v. Sims*, 471 U.S. 159 (1985). The Supreme Court, in reviewing a challenge to a classification decision under the National Security Act, 50 U.S.C. § 403-3, stated the policy of judicial review of classification decisions:

> [I]t is the responsibility of the Director of Central Intelligence, not the judiciary, to ***weigh*** the variety of complex and subtle factors in determining whether disclosure of information may lead to an ***unacceptable***

> risk of compromising the Agency's intelligence-gathering process. [emphasis added]. *Id.* at 180.

Sims discussion of "weighing...factors" to determine what risk to intelligence sources and gathering methods is "unacceptable" clearly infers some form of balancing test to be performed first by the CIA itself. Arabian Shield respectfully submits that one of the factors that must be weighed in the balance, under the governing language of E.O. 12958, is whether or not the information in question constitutes evidence of a crime. This, in fact, would appear to be the CIA's burden of proof under the FOIA and E.O. 12958 -- to demonstrate that is has considered and weighed all of the factors set out in E.O. 12958, including Section 1.8, in making its classification or declassification decision.

As has been stressed throughout this brief, the CIA cannot show the Court that it has done this task of weighing. The CIA does not know what, if anything, is contained in documents that might be responsive to Arabian Shield's FOIA requests. It has not looked.

And so, is there any balancing test, at least at the level of the CIA itself? As the matter now stands, under the ruling of the district and appellate courts, the answer is "no." Under the ruling of the district and appellate courts, once the CIA has determined that responding to an FOIA request may expose intelligence sources or methods of intelligence gathering, it need do nothing further. One must assume that much, perhaps most, of the intelligence gathered by the CIA is gathered from intelligence sources and through intelligence gathering methods. If even the CIA is not required to internally review its own materials, then Section 1.8 of E.O. 12958 becomes a hollow commandment.

IV. This Court should reverse the decision of the District and Appellate courts, remand this matter and order the CIA to conduct a balancing test pursuant to E.O. 12958.

Arabian Shield prays that the judgment of the trial court be reversed, and that this matter be remanded. However, Arabian Shield has never asked that information that the CIA deems sensitive be turned over to Arabian Shield. In its original pleadings, in status reports to the trial court, in its motion for summary judgment, Arabian Shield has consistently prayed for a graduated exploration into whatever information the CIA has in its possession.

Until the reply/response filed by the CIA in the summary judgment briefing process, Arabian Shield did not know that the CIA had not looked to see what documents might exist that might be responsive to Arabian Shield's FOIA request or that even the CIA was unaware of the content of any such documents. The Second Declaration of William H. McNair was the last document filed in that process. None of the prior filings by the CIA even hinted that it itself did not know the contents of responsive documents.

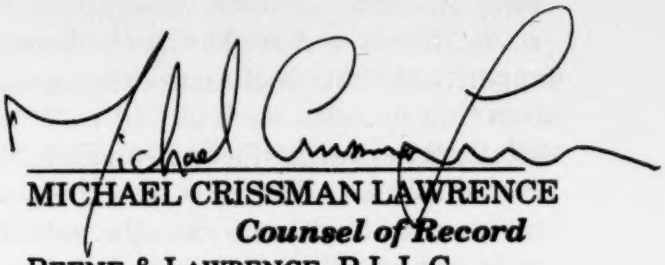
This one fact, the fact that the CIA has not looked as the FOIA, E.O. 12958, and, by implication, *CIA v. Sims, supra,* state it should, strongly suggests the first step has not occurred in any graduated approach to a remedy in this case. Arabian Shield prays that, upon remand, the trial court be instructed to order the CIA to review its own documents to determine what, if anything, can be released, perhaps in redacted or excerpted form, perhaps in the form of a partial release. An honest weighing of the contents of any such document review against the actual risk of compromising intelligence sources or gathering methodologies could possibly moot any other dispute in this matter.

CONCLUSION

This is a dispute in which one can find no cases supporting either position by the parties in the case. The cases that do exist, such as *CIA v. Sims, supra,* do not deal with the internal conflict within E.O. 12958 or with Section 1.8 of the Order. They do imply, however, a balancing and weighing test without directly holding that such a test needs to be applied in national security secrecy disputes. Section 1.8 of E.O. 12958 expresses a clear policy against using government secrecy in order to conceal a violation of law. It only has meaning when directed at the content of information in the hands of the CIA or other national security agency. If that content is not reviewed, even by the national security agency itself, then Section 1.8 cannot be used as a test for proper classification of intelligence information and would appear to become meaningless.

Since the CIA itself has not looked at the content of any documents that may be responsive to Arabian Shield's FOIA requests, it has not exercised its own expertise and discretion in determining whether the content of any such documents balances against the risks to intelligence sources or intelligence gathering methods. Arabian Shield prays that this matter be reversed and remanded to the trial court, with instructions that the CIA review its own documents to determine what, if any information, may or may not be at variance with Section 1.8 of E.O. 12958, and to assess the risks to intelligence sources or gathering techniques if all or parts of the subject information, if any exists, is released to Arabian Shield.

Respectfully submitted,



MICHAEL CRISSMAN LAWRENCE
Counsel of Record
BEENE & LAWRENCE, P.L.L.C.
5949 Sherry Lane, Suite 800
Dallas, Texas 75225
TEL: (214) 346-2630
FAX: (214) 346-2631
Counsel of Record for Petitioner
Arabian Shield Development Co.

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

No. 99-10327
Summary Calendar
Civil Docket No. 3:98-CV-624-BD

U.S. COURT OF APPEALS
FILED
JAN 28 2000
CHARLES R. FULBRUGE III
CLERK

ARABIAN SHIELD DEVELOPMENT COMPANY,
Plaintiff-Appellant,

versus

CENTRAL INTELLIGENCE AGENCY,
Defendant-Appellee.

Appeal from the United States District Court
for the Northern District of Texas
USDC No. 3:98-CV-624-BD

Before JOLLY, JONES, and BENAVIDES, Circuit Judges.

PER CURIAM:*

Arabian Shield Development Company appeals the district court's order granting the CIA's motion for summary judgment. Arabian Shield sought judicial review of the CIA's decision denying Arabian Shield's requests for information under the Freedom of Information Act, 5 U.S.C. § 552 (FOIA). The CIA denied

*Pursuant to 5th Cir. R. 47.5, the court has determined that this opinion should not be published and is not precedent except under the limited circumstances set forth in 5th Cir. R.47.5.4.

the requests because it determined that the fact of the existence or nonexistence of the requested information was classified pursuant to Executive Order 12958, and would relate directly to information concerning intelligence sources and methods which the Director of Central Intelligence has the responsibility to protect from disclosure pursuant to the National Security Act of 1947, 50 U.S.C. § 403(d)(3). Thus, the information was exempt from disclosure under FOIA §§ 552 (b)(10) and (b)(3).

We have reviewed the record and find no reversible error. Arabian Shield has not shown that the district court erred in concluding that the CIA had met its burden of establishing an exemption under FOIA § 552(b)(1). See 5 U.S.C. § 552(a)(4)(B). Nor has Arabian Shield shown that the district court erred in concluding that the information was exempt from disclosure under FOIA § 552(b)(3). See Knight v. CIA, 872 F.2d 660 (5th Cir. 1989).

AFFIRMED.

s/Jolly s/Jones s/Benavides

United States Court of Appeals
Fifth Circuit
Office of the Clerk

Charles R. Fulbruge, III
CLERK

TEL. 504-589-6514
600 CAMP STREET
NEW ORLEANS, LA 70130

January 28, 2000

MEMORANDUM TO COUNSEL OR PARTIES LISTED BELOW

Regarding: Fifth Circuit Statement on Petitions for Rehearing or Rehearing En Banc
No: 99-10327 Arabian Shield Devel v. Central Intelligence
USDC No. 3:98-CV-624-BD

Enclosed is a copy of the court's decision, and judgment has been entered under FED. R. APP. P. 36. (However, the opinion may yet contain typographical or printing errors which are subject to correction).

FED. R.APP.P.'S 39 THROUGH 41, and 5TH CIR. RULES 35, 39, and 41 govern costs, rehearings, and mandates. **New 5th CIR. RULES 35.2.10 and 40 require that a copy of the opinion or order sought to be reviewed shall bound with the petition for rehearing or suggestion for rehearing en banc as an appendix but shall not be marked or annotated.** Please read carefully the Internal Operating Procedures (IOP's) following FED.R.APP.P. 40 and 5TH CIR. R.35 for a discussion of when a rehearing may be appropriate, the legal standards applied and sanctions which may be imposed if a nonmeritorious suggestion for en banc is made.

Direct Criminal Appeals. 5TH CIR. R.41 provides that a

motion for a stay of mandate under FED.R.APP.P.41 shall not be granted simply upon request. The petition must set forth good cause for a stay or clearly demonstrate a substantial question is to be presented to the Supreme Court. Otherwise, the motion may be denied and the mandate issued immediately.

Pro Se Cases. If you were unsuccessful in the district court and/or on appeal, and will be considering filing a petition for certiorari in the United States Supreme Court, you do not need to file a motion for stay of mandate under FED. R. APP. P. 41. The issuance of the mandate does not affect the time, or your right, to file such a petition.

The judgment entered provides that plaintiff-appellant pay to defendant-appellee the costs on appeal.

Sincerely,

CHARLES R. FULBRUGE III, Clerk

By: s/Deborah M. Graham
Deborah M. Graham, Deputy Clerk

Enclosure
Mr. John Kelley Vaughan
Mr. Michael Crissman Lawrence
Mr. Leonard Aaron Schaitman
Mr. Steve L. Frank

ORIGINAL

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
FEB 26 1999
NANCY DOHERTY, CLERK
By s/DJD
Deputy

ENTERED ON DOCKET
MAR 01 1999
U.S. DISTRICT CLERK'S OFFICE

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

ARABIAN SHIELD DEVELOPMENT COMPANY	§	
Plaintiff,	§	NO. 3-98-CV-0624-BD
VS.	§	
CENTRAL INTELLIGENCE AGENCY	§	
Defendant.	§	

JUDGMENT

For reasons stated in the memorandum opinion and order dated February 26, 1999, defendant's motion for summary judgment is granted and plaintiff's motion for summary judgment is denied. All claims against defendant are dismissed with prejudice. Costs of court are taxed

against plaintiff.

SO ORDERED.

DATED: February 26, 1999

s/ JEFF KAPLAN
JEFF KAPLAN
UNITED STATES MAGISTRATE JUDGE

Certified a true copy of an instrument
on file in my office on 4/20/99
NANCY HALL DOHERTY, Clerk,
U.S. District Court, Northern District of Texas
By s/Nancy Colster, Deputy

ORIGINAL

U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
FEB 26 1999
NANCY DOHERTY, CLERK
By s/DJD
Deputy

ENTERED ON DOCKET
MAR 01 1999
U.S. DISTRICT CLERK'S OFFICE

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

ARABIAN SHIELD DEVELOPMENT COMPANY	§	
Plaintiff,	§	NO. 3-98-CV-0624-BD
VS.	§	
CENTRAL INTELLIGENCE AGENCY	§	
Defendant.	§	

MEMORANDUM OPINION AND ORDER

Certified a true copy of an instrument
on file in my office on 4/20/99
NANCY HALL DOHERTY, Clerk,
U.S. District Court, Northern District of Texas
By s/Nancy Colster, Deputy

This case is before the Court on cross-motions for summary judgment. For the reasons stated herein, defendant's motion is granted and plaintiff's motion is denied.

I.

Plaintiff Arabian Shield Development Company and Hunt Oil Company submitted competing bids on a petroleum production sharing agreement with the former Yemen Arab Republic in the early 1980's. The contract was ultimately awarded to Hunt Oil. Plaintiff suspected that Hunt secured the bid through bribery and filed a complaint with the Department of Justice. The complaint alleges that Hunt conspired with unnamed Yemeni officials to violate the Foreign Corruption Practices Act.[1]

Plaintiff further believes that the Central Intelligence Agency was actively monitoring negotiations for the oil concession. On August 8, 1997, plaintiff requested certain documents from the CIA under the Freedom of Information Act, 5 U.S.C. § 552 ("FOIA"). The request seeks "copies of all cable and other written traffic from the CIA Station, in Sana'a, Yemen Republic by Mr. Matthew Gannon, and others of the Station, during November and December, 1980 through all 1981, regarding Hunt Oil Company's . . . negotiations with the Yemen Government. . ." and "all correspondance [sic] between Hunt's vice president, Mr. Thomas Meurer, and Mr. James Lilley of the CIA, in Washington, during November and December of 1980, and in 1981, relating to Hunt's application for the [production sharing agreement] in Yemen." (Def. Motion, App. at 26).

---

[1]The Foreign Corrupt Practices Act prohibits a domestic concern from paying, offering, or promising anything of value to a foreign official to influence a decision "in order to assist such domestic concern in obtaining or retaining business for or with, or directing business to, any person." *See* 15 U.S.C. § 78dd-2. A willful violation of the statute is a criminal offense punishable by a fine not to exceed $1 million and up to ten years imprisonment., *Id.* § 78ff-(a)

The CIA responded to this request on September 11, 1997. The agency said it could neither confirm nor deny the existence of records responsive to the FOIA request because "[such information. . . would be classified for reasons of national security under Executive Order 12958."[2] (Def. Motion, App. at 27). Plaintiff appealed that decision to the Agency Release Panel. On October 8, 1997, plaintiff filed a second FOIA request. This time plaintiff sought seven categories of documents, including CIA communications with such highly placed officials as the United States Ambassador to South Korea, the former Prime Minister of Yemen, and then-Vice President George Bush. (Def. Motion, App. at 41-43).

The CIA affirmed its decision with respect to the first FOIA request on January 23, 1998. Specifically, the Agency Release Panel determined that:

> the fact of the existence or nonexistence of any documents which would be responsive to your request is classified pursuant to Executive Order 12958. Further, the fact of the existence or nonexistence of such documents would relate directly to information concerning intelligence sources and methods which the Director of Central Intelligence has the responsibility to protect from unauthorized disclosure in accordance with Subsection 102(d)(3) of the National Security Act of 1949. Accordingly, pursuant to Freedom of Information Act exemptions (b)(1) and (b)(3), your appeal is

---

[2]The refusal to confirm or deny the existence of documents is known as a "Glomar response." The term comes from a case involving the *Hughes Glomar Explorer*, a research ship used by the government to conduct secret operations. *See Phillippi v. Central Intelligence Agency*, 546 F.2d 1009, 1010-11 (D.C.Cir. 1976).

denied.

(Def. Motion, App. at 39-40).

Plaintiff filed the instant lawsuit to obtain judicial review of the agency's decision and compel the production of documents specified in its first FOIA request. While this case was pending, the CIA issued a final decision with respect to plaintiff's second FOIA request. The agency refused to confirm or deny the existence of any responsive documents for the same reasons cited in support of its earlier decision. (Def. Motion, App. at 59-61). Thereafter, plaintiff amended its complaint to include its second FOIA request.[3]

Both parties now move for summary judgment. Defendant maintains that it properly refused to confirm or deny the existence of documents responsive to plaintiff's requests under certain exemptions to FOIA. Plaintiff argues that these exemptions cannot be used to conceal evidence of a crime. The issues have been fully briefed and argued by the parties, and this matter is ripe for determination.

II.

The burden of establishing an exemption under FOIA rests with the agency resisting disclosure. 5 U.S.C. § 552(a)(4)(B); *Minier v. Central Intelligence Agency*, 88 F.3d 796, 800 (9th Cir. 1996); *Miller v. Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984). The Court reviews the agency's decision *de novo*. 5 U.S.C. § 552(a)(4)(B); *Miller*, 730 F.2d at 776. Nevertheless, "Executive departments responsible for national defense and foreign policy matters have unique

---

[3]Plaintiff also filed two other FOIA requests on March 5, 1998 and March 10, 1998. Leave to add these requests to the pending lawsuit was denied because plaintiff has not exhausted its administrative remedies. *See Dresser Industries, Inc. v. United States*, 596 F.2d 1231, 1238 (5th Cir. 1979), *cert. denied*, 100 S.Ct. 731 (1980); *Hedley v. United States*, 594 F.2d 1043, 1044 (5th Cir. 1979).

insights into what adverse affects [sic] might occur as a result of public disclosures of a particular classified record." *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981), *quoting* S. Rep. No. 93-1200, 93d Cong., 2d Sess. 12 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6267, 6290. Therefore, the Court is required to "accord substantial weight to an agency's affidavit concerning the details of the classified status of the disputed record." *Id.* The agency is entitled to summary judgment where its affidavits (1) describe the justifications for nondisclosure in reasonably specific detail; (2) demonstrate that the information withheld logically falls within the claimed exemption; and (3) are not controverted by contrary evidence in the record or evidence of agency bad faith. *Miller*, 730 F.2d at 776; *Military Audit Project*, 656 F.2d at 738.

A.

Defendant relies on two FOIA exemptions to support the denial of plaintiff's requests. The first exemption applies to matters that are "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive order." 5 U.S.C. § 552(b)(1). Executive Order 12958 provides that information may be classified if four conditions are met: (1) an original classification authority is classifying the information; (2) the information is owned by, produced by or for, or is under the control of the United States government; (3) the information falls within one or more of the categories listed in section 1.5 of the order;[4] and (4) the classification authority determines

---

[4]Section 1.5 provides that "[i]nformation may not be considered for classification unless it concerns:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United

that disclosure of the information reasonably could be expected to damage national security and identifies or describes the damage. Exec. Order 12958 § 1.2, 1995 WL 231453 (April 17, 1995).

William H. McNair, Information Review Officer for the Directorate of Operations, has submitted a detailed affidavit in support of defendant's motion for summary judgment. McNair states that he holds original classification and declassification authority under Executive Order 12958. (Def. Motion, App. at 2, ¶ 3). It is clear from the face of the FOIA requests that any responsive documents, to the extent that such documents even exist, were produced by or for the United States government. The CIA determined that the requested information concerned intelligence activities, intelligence sources or methods, and foreign relations or foreign activities of the United States. (Def. Motion, App. at 22, ¶¶ 44-45). Therefore, the information is subject to classification under the Executive Order. Exec. Order 12958 §§ 1.5(c) & (d).

McNair further explains why disclosure of the information would damage national security. Plaintiff requested documents reflecting communications between the CIA, various foreign government officials, and Hunt Oil Company that concerned specific activities occurring in Yemen. The agency determined that acknowledging whether such documents exist would reveal: (1) whether the CIA has an intelligence relationship with, or an intelligence interest in, the named individuals and

---

States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States government programs for safeguarding nuclear materials or facilities; or

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security."

Exec. Order 12958 §1.5.

corporations; (2) whether particular individuals are employed by the CIA; (3) whether the agency maintains a facility in Sana'a Yemen; and (4) whether the CIA has an intelligence interest in the petroleum production sharing agreement that was awarded to Hunt Oil. (Def. Motion, App. at 8-9, ¶ 23). McNair states that disclosure of this information would damage national security. (Def. Motion, App. at 20-21, ¶ 41). Moreover, revealing that the agency has collected intelligence regarding specific individuals or corporations, or has an intelligence interest or a facility in a particular foreign location, could trigger a negative diplomatic or economic response or invite retaliation against American interests in that country. (Def. Motion, App. at 22-23, ¶¶ 44-45). McNair explains that it would not be difficult for a hostile intelligence agency to use such information to identify current covert CIA stations and employees. This would put the lives of covert operatives and their families at risk and deter others from cooperating in the agency's intelligence-gathering efforts. (Def. Motion, App. at 11-13, ¶¶ 26-29, 32, 33).[5]

The Court finds the evidence sufficient to demonstrate that defendant properly classified the requested information under Executive Order 12958 and properly refused to confirm or deny the existence or nonexistence of documents specified in the FOIA requests.

---

[5]The affidavit of Hatem El-Khalidi recites that Matthew Gannon and James Lilley were both acknowledged as CIA agents in unspecified public news reports. (Plf. Motion, App. At 15). Plaintiff therefore maintains that such information cannot be classified as a matter of law. This argument was raised for the first time at the summary judgment hearing and should be rejected for that reason alone. Moreover, public speculation and disclosure regarding CIA affiliations is quite different from official confirmation. *See Fitzgibbon v. Central Intelligence Agency,* 911 F.2d 755, 765-66 (D.C.Cir. 1990); *Alfred A. Knopf, Inc. v. Colby,* 509 F.2d 1362, 1370-71 (4th Cir.), *cert. denied,* 95 S.Ct. 1999 (1975). The agency may be compelled to disclose information only when it has been "officially acknowledged." *See Fitzgibbon,* 911 F.2d at 765, *citing Afshar v. Department of State,* 702 F.2d 1125, 1133 (D.C.Cir. 1983).

See Exec. Order 12598 § 3.7(a) (agency may refuse to confirm or deny existence or nonexistence of records when "the fact of existence or nonexistence is itself classified under this order"). Defendant has adequately explained its reasons for not disclosing the information and shown that the document requests are exempt under FOIA. *Miller*, 730 F.2d at 776.

Plaintiff argues that the requested information was improperly classified by the CIA because "national security secrecy cannot be used to conceal information pertaining to the commission of a crime . . ." (Plf. Motion at 1). However, a careful reading of the Executive Order compels a different conclusion. The order provides that "[i]n no case shall information be classified *in order to* . . . conceal violations of law, inefficiency, or administrative error." Exec. Order 12958 §1.8(a)(1) (emphasis added). Section 1.8 thus prohibits an agency from classifying documents as a ruse when they could not otherwise be withheld from public disclosure. It does not prevent the classification of national security information merely because it might *reveal* criminal or tortious acts. Plaintiff has neither argued nor offered evidence that the CIA classified the requested information for the purpose of concealing a crime. Therefore, defendant acted in accordance with the Executive Order.

B.

The second FOIA exemption cited by defendant applies to matters that are "specifically exempted from disclosure by statute . . . provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C.§ 552(b)(3). The CIA refused to confirm nor deny the existence of information requested by plaintiff pursuant to the National Security act of 1947 and the Central Intelligence Agency Act of 1949. (Def. Motion, App. at 39-40, 59-61). Both statutes qualify as "withholding statues"

for purposes of the (b)(3) exemption. *See Minier*, 88 F.3d at 801. Because case law involving the National Security Act is more thoroughly developed, the Court will focus on that statute.

The National Security Act vests the Director of Central Intelligence with responsibility for protecting intelligence-gathering activities from unauthorized disclosure. 50 U.S.C. § 403-3(c)(6). In order to claim the protection of the Act, the CIA must demonstrate that an answer to plaintiff's FOIA request could reasonably be expected to lead to the unauthorized disclosure of intelligence sources and methods. *Gardels v. Central Intelligence Agency,* 689 F.2d 1100, 1103 (D.C. Cir. 1982). However, the Director's determination in this regard is almost unassailable. The unique nature of the agency's mandate gives it broad power to protect intelligence sources and methods. *Central Intelligence Agency v. Sims,* 471 U.S. 159, 168-69, 105 S.Ct. 1881, 1887-88, 85 L.Ed.2d 173 (1985). "[I]t is the responsibility of the Director of Central Intelligence, not of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence-gathering process." *Id.* At 1893-94. Absent evidence of bad faith, the agency's determination "is beyond the purview of the courts." *Knight v. United States Central Intelligence Agency,* 872 F.2d 660, 664 (5th Cir. 1989), *cert. denied,* 110 S.Ct. 1296 (1990).

Plaintiff does not suggest that the CIA is guilty of bad faith. Instead, it contends that the agency should not be permitted to conceal evidence of crime by classifying documents that are otherwise protected under the National Security Act. Plaintiff admits that the statute contains no such exception, but argues that the legislative history of a parallel statute "point[s] to the conclusion that CIA secrecy cannot be used to conceal information pertaining to the

commission of a crime. (Plf. Motion at 2).[6] The Court disagrees. The plain meaning of the statute "may not be squared with any limiting definition that goes beyond the requirement that the information fall within the Agency's mandate to conduct foreign intelligence." *Sims,* 105 S.Ct. at 1888. Courts have recognized that this interpretation of the National Security Act is "only a short step [from] exempting all CIA records from FOIA." *Hunt v. Central Intelligence Agency,* 981 F.2d 1116, 1120 (9th Cir. 1992). Nevertheless, Congress has not elected to abridge the broad powers granted to the Director. This Court declines to do so by judicial fiat.

For these reasons, defendant's motion for summary judgement is granted and plaintiff's motion is denied. The Court will enter a final judgment in favor of defendant by separate order.

SO ORDERED.

DATED: February 26, 1999.

s/ JEFF KAPLAN

---

[6]The "parallel statute" cited by plaintiff is the Central Intelligence Act of 1984, 50 U.S.C. § 431. The general intent of this statute is to exempt CIA operational files from FOIA review. *Id.* § 431(a). However, there is an exception for operational files regarding, *inter alia*, Department of Justice investigations of "any impropriety, or violation of law. . . in conduct of an intelligence activity." *Id.* § 431(c). Plaintiff notes that this statute, unlike the National Security Act, was enacted after FOIA. Therefore, plaintiff reasons that the statute "clearly demonstrates that Congress, in general, does not contemplate using national security as a device for concealing information of a crime." (Plf. Motion at 8).

Even accepting this contorted argument on its own terms, it does not support plaintiff's conclusion. The statute specifically refers to improprieties "in the conduct of an intelligence activity." 50 U.S.C. § 431(c). Plaintiff presents no evidence or argument that the CIA conducted its intelligence activities in an improper or illegal manner.

JEFF KAPLAN
UNITED STATES MAGISTRATE JUDGE

Arabian Shield Development Company
10830 North Central Expressway, Suite 175
Dallas, Texas 75231
(214) 692-7872

August 8, 1997

Information & Privacy Coordinator
Office of Information Services
Central Intelligence Agency
Washington, D.C. 20505

Dear Sir:

In accordance with the provisions of the Freedom of Information Act, 5 U.S.C. 552, we are requesting copies of all cable and other written traffic from the CIA Station, in Sana'a, Yemen Republic by Mr. Matthew Gannon, and others of the Station, during November and December, 1980 through all 1981, regarding Hunt Oil Company's ("Hunt") negotiations with the Yemen Government, in association with the CIA, in order to obtain a petroleum production sharing agreement ("PSA"), for the Ma'arib Basin in northeast Yemen, which PSA was subsequently awarded to it in late 1981.

Also requested is all correspondence between Hunt's vice president, Mr. Thomas Meurer, and Mr. James Lilley of the CIA, in Washington, during November and December of 1980, and in 1981, relating Hunt's application for the PSA in Yemen. In Mr. Meurer's sworn deposition to the Dallas County Court (116th Judicial District), Texas, in Case No. 87-13271-F, on March 2, 1988, he indicated that he consulted only with Mr. Lilley in December, 1980, prior to his trip to Yemen on January 2, 1981, in pursuit of the PSA. A blind copy of Mr. Meurer's report of his trip to Yemen, dated January 15, 1981, was sent to Mr. Lilley.

This requested information will be presented to the U.S. Department of Justice ("DOJ"), as evidence in this

Company's complaint to the DOJ, dated May 15, 1991, which is still extant, regarding Hunt's conspiracy to violate the Foreign Corrupt Practices Act, and that is for the purpose of excluding this Company's offer for the PSA for the same area, which was made before Hunt's. The result of the conspiracy was the summary exclusion of this Company's offer by the Yemen Government, and the subsequent granting of the PSA to Hunt in late 1981.

This Company is a US public stock company (Delaware corporation), traded on NASDAQ since its formation in 1967, and operating in the USA and the Near East. I am a USA citizen, and my social security number is: 386-32-7689. Thank you.

Very truly yours,
ARABIAN SHIELD DEVELOPMENT COMPANY
s/Hatem El-Khalidi

By: Hatem El-Khalidi, President & CEO

Central Intelligence Agency
[Seal: Central Intelligence Agency]
Washington, DC 20505

23 JAN 1998

Mr. Hatem El-Khalidi
President and CEO
Arabian Shield Development Company
10830 North Central Expressway, Suite 175
Dallas, Texas 75231

Reference: F97-1889

Dear Mr. El-Khalidi:

This is in response to your 16 September 1997 letter in which you appealed the 11 September 1997 determination of this Agency in response to your 8 August 1997 Freedom of Information Act request for:

> ". . . all cable and other written traffic from the CIA Station, in Sana'a, Yemen Republic by Mr. Matthew Gannon, and others of the Station, during November and December, 1980 through 1981, regarding Hunt Oil Company's ("Hunt") negotiations with the Yemen Government, in association with the CIA, in order to obtain a petroleum production sharing agreement ("PSA"), for the Ma'arib Basis in northeast Yemen, which PSA was subsequently awarded to it in late 1981.
>
> Also requested is all correspondence between Hunt's vice president, Mr. Thomas Meurer, and Mr. James Lilley of the CIA, in Washington, during November and December of 1980, and in

1981, relating to Hunt's application for the PSA in Yemen. . . ."

Specifically, you appealed our determination neither to confirm nor deny the existence or nonexistence of records responsive to your request on the basis of Freedom of Information Act exemptions (b)(1) and (b)(3).

Your appeal has been presented to the appropriate member of the Central Intelligence Agency Release Panel, Mr. William H. McNair, Information Review Officer for the Directorate of Operations. Pursuant to the authority delegated under paragraph 1900.51(a) of Chapter XIX, Title 32 of the Code of Federal Regulations, Mr. McNair has determined that the fact of the existence or nonexistence of any documents which would be responsive to your request is classified pursuant to Executive Order 12958. Further, the fact of the existence or nonexistence of such documents would relate directly to information concerning intelligence sources and methods which the Director of Central Intelligence has the responsibility to protect from unauthorized disclosure in accordance with Subsection 102 (d) (3) of the National Security Act of 1947 and Section 6 of the Central Intelligence Agency Act of 1949. Accordingly, pursuant to Freedom of Information Act exemptions (b)(1) and (b)(3), your appeal is denied. By this statement, we are neither confirming nor denying that any such documents exist. Further, in regard to your appeal and in accordance with CIA regulations appearing at 32 C.F.R. paragraph 1900.51(b), the Agency Release Panel, meeting as a committee of the whole, has affirmed this determination.

In accordance with the provisions of the Freedom of Information Act, you have the right to seek judicial review of the above determination in a United States district court.

We appreciate your patience while your appeal was being considered.

Sincerely,

s/EDC

Edmund Cohen
Chairman
Agency Release Panel

Arabian Shield Development Company
10830 North Central Expressway, Suite 175
Dallas, Texas 75231
(214) 692-7872

IPCRD NO.
F-1997-02491
RPM
October 8, 1997

Information and Privacy Coordinator
Office of Information Services
Central Intelligence Agency
Washington, D.C. 20505

14 OCT'97 PM 1:

Dear Sir:

In accordance with the Provisions of the Freedom of Information Act, 5 U.S.C. 552, we request the following:

1. Copies of all communications from Mr. Matthew Gannon, of the CIA, to the CIA, after his telephone conversation, on August 31, 1987, with this Company's attorney, H. Dee Johnson Jr., Esquire, regarding Hunt Oil Company's("Hunt") operations in Yemen, in 1981, when Mr. Gannon was attached to the US Embassy there, during that year (1981).

2. Copies of all communications between the CIA and Mr. Lawrence Eagleburger, President of Kissinger & Associates, during January-June, 1988, concerning his preparation of an affidavit dated June 29, 1988, which he presented to the Court, in the case of Hunt vs. Dorchester/Arabian (Case no: 87-13271-F, in the District Court of Dallas County, Texas, 116th Judicial District). In the affidavit, Mr. Eagleburger expressed deceptive opinions as to why this Company could not have been granted the petroleum production sharing agreement ("PSA"), for which it had applied, in the Marib Basin in Yemen, in 1981.

3. Copies of all communications between Sheikh Kamal Adham of Saudi Arabia, and the CIA during 1980-1981,

regarding this Company's application for the PSA mentioned above, and any subsequent communications regarding that matter, following the filing of this Company's law suit in the Texas Court, mentioned above, on October 2, 1987.

4. Copies of all communications between Mr. James Lilley, U.S. Ambassador to South Korea, and the CIA, during 1987-1988, regarding this Company's law suit, mentioned above, filed in the Texas Court on October 2,1987. Sometime during that period, Mr. Lilley and the CIA were asked by Hunt to try to find derogatory information about one of this Company's investigators, Mrs. Ann Cardash. Mr. Lilley contacted Mr. Calvin White, then Treasury Attache at the Embassy. Mrs. Cardash had previously worked as an informant for Mr. White when he was attached to the U.S. Embassy in London, England. After Ambassador Lilley contacted Mr. White, seeking that information, Mr. White telephoned Mrs. Cardash and reported the above to her.

5. Copies of all communications during 1981 between Vice President George Bush and Mr. James Lilley of the CIA, and other officials of the CIA, regarding Hunt's application for, and the winning of the PSA mentioned above, in Yemen in 1981.

6. Copies of all communications during 1981, between Hunt, the CIA, Vice President Bush, and Dr. Abdul Kerim El-Eryani, then Prime Minister of Yemen, and a CIA 'asset', who is known to be the most corrupt politician in Yemen, regarding helping Hunt in its application and obtaining the PSA mentioned above after excluding this Company. Dr. El-Eryani was recruited by the CIA during his stay in the US as a student, and returned to Yemen in 1968, after obtaining his Ph.D. from Yale University. Also requested are copies of all communications between Dr. El-Eryani, the CIA and Hunt, regarding the presentation of an affidavit by Dr. El-Eryani to the Texas Court mentioned above, dated November 15, 1988, in which he committed perjury, in a conspiracy with Hunt to cover up the forged signatures of

the ex-minister of petroleum, Ali Al-Bahr, on two affidavits supposedly from the ex-minister, presented by Hunt to the Texas Court.

7. Copies of all communications regarding the transfer of $100,000 during 1981, from the CIA to Hunt, which amount was then paid by check no: 10008 from Hunt's account, into the account of Manar Al-Malazi, the brother of Hunt's go-between, Moujib Al-Malazi, account no: 458-S, in the Banca Populare Di Modena, in Modena, Italy, on December 7, 1981. Subsequently this same amount ($100,000) was transferred on February 17, 1982, into the account of the shell Panamanian company, MAM International, formed by Moujib Al-Malazi, in the Swiss Bank Corporation, account no: C-6-102, 455.

The above requested communications, in the form of letters, reports, and memoranda are needed because they contain evidence, which will be presented to the US Department of Justice ("DOJ"), in order to prove this Company's allegations presented in the complaint to the DOJ on May 15, 1991, which is still extant, that Hunt and others, including Yemeni officials, among whom was Dr. El-Eryani, and go-betweens, with the knowledge and association of the CIA, were engaged in a conspiracy to, and violation of the Foreign Corrupt Practices Act, in order to exclude the application of this Company and Dorchester Gas Company, both US public stock corporations with thousands of US shareholders, for the PSA in the Marib Basin in Yemen, during 1981.

We are willing to pay any fees which may be required to satisfy our request. If our requests for the above information is denied, we plan to make an appeal to your Agency Release Panel.

This Company is a US public stock corporation (Delaware), traded on NASDAQ (Symbol ARSD), since its formation in 1967, and operating in the USA and the Near East. I am a USA citizen, and my social security number is 386-32-7689.

May we respectfully request that your response to our request in this letter be sent to us within 10 working days after you receive it. Thank you for your cooperation.

Very truly yours,

ARABIAN SHIELD DEVELOPMENT COMPANY

s/Hatem El-Khalidi

By: Hatem El-Khalidi, President & CEO

JUN 30 1999

Mr. Hatem El-Khalidi
President & CEO
Arabian Shield Development Company
10830 North Central Expressway, Suite 175
Dallas, Texas 75231

Reference: F-19997-02491

Dear Mr. El-Khalidi:

This is in response to your letter of 20 January 1998 in which you appealed the 8 January 1998 determination of this Agency in response to your 8 October 1997 Freedom of Information Act request for the following:

> "1. Copies of all communications from Mr. Matthew Gannon, of the CIA, to the CIA, after his telephone conversation, on August 31, 1987, with [your] company's attorney, H. Dee Johnson, Jr., Esquire, regarding Hunt Oil Company's ("Hunt") operations in Yemen, in 1981....
>
> 2. Copies of all communications between the CIA and Mr. Lawrence Eagleburger, President of Kissinger & Associates, during January-June, 1988, concerning his preparation of an affidavit dated June 29, 1988, which he presented to the Court, in the case of Hunt vs. Dorchester/Arabian (Case No. 897-13271-F, in the District Court of Dallas County Texas, 116th Judicial District). In the affidavit, Mr. Eagleburger expressed

deceptive opinions as to why this Company could not have been granted the petroleum production sharing agreement ('PSA'), for which it had applied, in the Marib Basin in Yemen, in 1981.

3. Copies of all communications between Sheikh Kamal Adham of Saudi Arabia, and the CIA during 1980-1981, regarding this Company's application for the PSA mentioned above, and any subsequent communications regarding that matter, following the filing of this Company's lawsuit in the Texas Court, mentioned above, on October 2, 1987.

4. Copies of all communications between Mr. James Lilley, U.S. Ambassador to South Korea, and the CIA, during 1987-1988, regarding this Company's Lawsuit, mentioned above, filed in the Texas Court on October 2,1987....

5. Copies of all communications during 1981, between Vice President George Bush and Mr. James Lilley of the CIA, and other officials of the CIA, regarding Hunt's application for, and the winning of the PSA mentioned above, in Yemen in 1981.

6. Copies of all communications during 1981, between Hunt, the CIA, Vice President George Bush and Dr. Abdul Karim El-Eryani, then Prime Minister of Yemen...regarding helping Hunt in its application and obtaining the PSA mentioned above after excluding this Company....Also requested are copies of

all communications between Dr. El-Eryani, the CIA and Hunt, regarding the presentation of an affidavit by Dr. El-Eryani to the Texas Court mentioned above, dated November 15, 1988, in which he committed perjury, in a conspiracy with Hunt to cover up the3 forged signatures of the ex-minister of petroleum, Ali-Bahr, on two affidavits supposedly from the ex-minister, presented by Hunt to the Texas Court.

7. Copies of all communications regarding the transfer of $100,000 during 1981, from the CIA to Hunt, which amount was then paid by check no. 10008 from Hunt's account, into the account of Manar Al-Malazi, the brother of Hunt's go-between, Moujib Al-Malazi, account no. 548-S, in the Banca Populare Di Modena, in Modena, Italy, on December 7, 1981...."

Specifically, you appealed our determination to neither confirm nor deny the existence or nonexistence of records responsive to your request on the basis of Freedom of Information Act exemptions (b)(1) and (b)(3).

Your appeal has been presented to the appropriate member of the Agency Release Panel, Mr. William H. McNair, Information Review Officer for the Directorate of Operations. Pursuant to the authority delegated under paragraph 1900.43 of Chapter XIX, Title 32 of the Code of Federal Regulations (C.F.R.), Mr. McNair has determined that the fact of the existence or nonexistence of any documents which would be responsive to your request is classified pursuant to Executive Order 12958. Further, the fact of the existence or nonexistence of such documents would relate directly information concerning intelligence

sources and methods which the Director of Central Intelligence has the responsibility to protect from unauthorized disclosure in accordance with Subsection 103(c)(5) of the National Security Act of 1949. Accordingly, pursuant to Freedom of Information Act exemptions (b)(1) and (b)(3), your appeals is denied. By this statement, we are neither confirming nor denying that any such documents exist.

Further, in regard to your appeal and in accordance with CIA regulations appearing at 32 C.F.R. paragraph 1900.41(c)(2), the Agency Released Panel, meeting as a committee of the whole, has affirmed this determination.

We appreciate your patience while your appeal was being considered.

Sincerely,
ORIGINAL SIGNED
Edmund Cohen
Chairman
Agency Release Panel

5 U.S.C. § 552. Public Information; agency rules, opinions, orders, records, and proceedings

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public—

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when

incorporated by reference therein with the approval of the Director of the Federal Register.

(2) Each agency, in accordance with published rules, shall make available for public inspection and copying—

(A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

(B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register; and

(C) administrative staff manuals and instructions to staff that affect a member of the public;

unless the materials are promptly published and copies offered for sale. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction. However, in each case the justification for the deletion shall be explained fully in writing. Each agency shall also maintain and make available for public inspection and copying current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly publish, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplements thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of such index on request at a cost not to exceed the direct cost of duplication. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a

member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if—

(i) it has been indexed and either made available or published as provided by this paragraph; or

(ii) the party has actual and timely notice of the terms thereof.

(3) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, each agency, upon any request for records which (A) reasonably describes such records and (B) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

(4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing or requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.

(ii) Such agency regulations shall provide that—

(I) fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use;

(II) fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; or a representative of

the news media; and

(III) for any request not described in (I) or (II), fees shall be limited to reasonable standard charges for document search and duplication.

(iii) Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii) If disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.

(iv) Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review. Review costs shall include only the direct costs incurred during the initial examination of a document for the purposes of determining whether the documents must be disclosed under this section and for the purposes of withholding any portions exempt from disclosure under this section. Review costs may not include any costs incurred in resolving issues of law or policy that may be raised in the course of processing a request under this section. No fee may be charged by any agency under this section—

(I) if the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee; or

(II) for any request described in clause (ii)(II) or (III) of this subparagraph for the first two hours of search time or for the first one hundred pages of duplication.

(v) No agency may require advance payment of any fee unless the requester has previously failed to pay fees in a timely fashion, or the agency has determined that the fee will exceed $250.

(vi) Nothing in this subparagraph shall supersede fees chargeable under a statute specifically providing for setting the level of fees for particular types of records.

(vii) In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo: *Provided,* That the court's review of the matter shall be limited to the record before the agency.

(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action.

(C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under this subsection within thirty days after service upon the defendant of the pleading in which such complaint is made, unless the court otherwise directs for good cause shown.

[**(D)** Repealed. Pub.L.98-620, Title IV, § 402(2), Nov.8, 1984, 98 Stat. 3357]

(E) The court may access against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.

(F) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding

the withholding raise questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding. The Special Counsel, after investigation and consideration of the evidence submitted, shall submit his findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his representative. The administrative authority shall take the corrective action that the Special Counsel recommends.

(G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.

(5) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

(6)(A) Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall—

(i) determine within ten days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency any adverse determination; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this

subsection.

(B) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the reasons for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days. As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular request—

> **(i)** the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;
>
> **(ii)** the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or
>
> **(iii)** the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject-matter interest therein.

(C) Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails to comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records. Upon any determination by an agency to comply with a request for

records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.

(b) This section does not apply to matters that are—

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B)are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria of withholding or refers to particular types of matters to be withheld;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement

proceedings, (B) would deprive a person of a right to a fair trail or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E)(would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.

(c)(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and—

(A) the investigation or proceeding involves a possible violation of criminal law;

and

(B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could be reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.

(2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.

(3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

(d) This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.

(e) On or before March 1 of each calendar year, each agency shall submit a report covering the preceding calendar year to the Speaker of the House of Representatives and President of the Senate for referral to the appropriate committees of the Congress. The report shall include—

(1) the number of determinations made by such

agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;

(2) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information;

(3) the names and titles or positions of each person responsible for the denial of records requested under this section, and the number of instances of participation for each;

(4) the results of each proceeding conducted pursuant to subsection (a)(4)(F), including a report of the disciplinary action taken against the officer or employee who was primarily responsible for improperly withholding records or an explanation of why disciplinary action was not taken;

(5) a copy of every rule made by such agency regarding this section;

(6) a copy of the fee schedule and the total amount of fees collected by the agency for making records available under this section; and

(7) such other information as indicates efforts to administer fully this section.

The Attorney General shall submit an annual report on or before March 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subsections (a)(4)(e), (F), and (G). Such report shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.

(f) For purposes of this section, the term "agency" as

defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

(Pub.L. 89-554, Sept. 6, 1966, 80 Stat. 383; Pub.L. 90-23, § 1, June 5, 1967, 81 Stat. 54; Pub.L. 93-502, §§ 1 to 3, Nov.21, 1974, 88 Stat. 1561 to 1564; Pub.L. 94-409, § 5(b), Sept. 13, 1976, 90 Stat. 1247; Pub.L. 95-454, Title IX, § 906(a)(10), Oct. 13, 1978, 92 Stat. 1225; Pub.L. 98-620, Title IV, § 402(2), Nov. 8, 1984, 98 Stat. 3357; Pub.L. 99-570, Title I, §§ 1802, 1803, Oct. 27, 1986, 100 Stat. 3207-48, 3207-49.)

Executive Order 12958
Classified National Security Information
April 17, 1995

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

NOW, THEREFORE, by the authority vested in me as President, by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1--ORIGINAL CLASSIFICATION

Sec. 1.1. Definitions. For purposes of this order:

(a) "National security"means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is

marked to indicate its classified status when in documentary form.

(d) "Foreign Government Information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

(j) "Senior agency official" means the official designated by the agency head under section 5.6(c) of this order to

direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Sec. 1.2. Classification Standards. (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of

identical or similar information.

Sec. 1.3. Classification Levels. (a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.4. Classification Authority. (a) The authority to classify information originally may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; or

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for

ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the

information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.5. Classification Categories.

Information may not be considered for classification unless it concerns:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Sec. 1.6. Duration of Classification. (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

(1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair the development or use of technology within a United States weapons system;

(4) reveal United States military plans, or national security emergency preparedness plans;

(5) reveal foreign government information;

(6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;

(7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or

(8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.7. Identification and Markings. (a) At the time of original classification, the following shall appear on the

face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.3 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or

(C) the exemption category from declassification, as prescribed in section 1.6(d); and

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Sec. 1.8. Classification Prohibitions and Limitations . (a) In no case shall information be classified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the

Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information.

As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.9. Classification Challenges. (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

PART 2--DERIVATIVE CLASSIFICATION

Sec. 2.1. Definitions. For purposes of this order:

(a) "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

Sec. 2.2. Use of Derivative Classification. (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification

authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.3. Classification Guides. (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

PART 3--DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. Definitions. For purposes of this order:

(a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as

determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(c) "Declassification authority" means:

(1) the official who authorized the original classification, if that official is still serving in the same position;

(2) the originator's current successor in function;

(3) a supervisory official of either; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Sec. 3.2. Authority for Declassification. (a) Information shall be declassified as soon as it no longer

meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The

information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.3. Transferred Information. (a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above,

but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

Sec. 3.4. Automatic Declassification. (a) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1)

are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

(1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;

(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

(8) reveal information that would seriously and

demonstrably impair current national security emergency preparedness plans; or

(9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the file series;

(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the information;

(2) an explanation of why the information is exempt from automatic declassification and must remain

classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year fromthe effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

Sec. 3.5. Systematic Declassification Review. (a) Each agency that has originated classified information

under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central

Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.6. Mandatory Declassification Review. (a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and

(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary

subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Sec. 3.7. Processing Requests and Reviews. In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the

existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.8. Declassification Database. (a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Governmentwide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

PART 4--SAFEGUARDING

Sec. 4.1. Definitions. For purposes of this order: (a) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(b) "Access" means the ability or opportunity to gain knowledge of classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a

prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers that can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Sec. 4.2. General Restrictions on Access. (a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from

official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided bystatute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific

information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Sec. 4.3. Distribution Controls. (a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need- to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.4. Special Access Programs. (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or

(3) the program is required by statute.

(b) Requirements and Limitations. (1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably

small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

(c) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.5. Access by Historical Researchers and Former Presidential Appointees. (a) The requirement in section 4.2(a)(3) of this order that access to classified

information may be granted only to individuals who have a need- to-know the information may be waived for persons who:

(1) are engaged in historical research projects; or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

PART 5--IMPLEMENTATION AND REVIEW

Sec. 5.1. Definitions. For purposes of this order: (a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the

requirements of this order.

(c) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation," as defined above.

Sec. 5.2. Program Direction. (a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

(1) classification and marking principles;

(2) agency security education and training programs;

(3) agency self-inspection programs; and

(4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

Sec. 5.3. Information Security Oversight Office. (a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of

Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the

program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.4. Interagency Security Classification Appeals Panel.

(a) Establishment and Administration.

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) Functions. The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.4 of

this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

(c) Rules and Procedures. The Panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which: (1) the appellant has exhausted his or her administrative remedies within the responsible agency; (2) there is no current action pending on the issue within the federal courts; and (3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

Sec. 5.5. Information Security Policy Advisory Council.

(a) Establishment. There is established an Information Security Policy Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from

among persons who have demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. 2.

(b) Functions. The Council shall:

(1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this order or its implementing directives, including recommended changes to those policies;

(2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) Meetings. The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) Administration.

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) To the extent permitted by law and subject

to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Sec. 5.6. General Responsibilities. Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order; and

(c)designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.7. Sanctions. (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate

holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2)or (3), above, occurs.

PART 6--GENERAL PROVISIONS

Sec. 6.1. General Provisions. (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Sec. 6.2. Effective Date. This order shall become effective 180 days from the date of this order.

s/WILLIAM J. CLINTON
THE WHITE HOUSE,
April 17, 1995.